

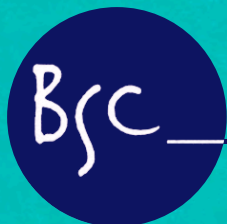
PROTECT

Your Identity, Money
& Information!

How to Spot and Deal with

SCAMS

FIRST EDITION



ADDING LIFE TO THE YEARS

Brookline Senior Center



January 2025

Brookline Council on Aging

We are pleased to provide the first edition of **Protect Your Identity, Money & Information! How to Spot and Deal with Scams** to our community. Thanks to the generosity of donors and sponsors, we are able to distribute this publication without cost, and provide older adults with significant information that is both preventative and practical. Scams are an increasing problem - defrauding our older adults nearly \$10 million daily, according to the FBI Internet Crime Complaint Center. We truly believe that the best defense is to stay informed and be alert to how scammers operate.

We hope that you will find this publication to be helpful. We also encourage our residents to reach out to the Council on Aging social worker of the day at 617-730-2777, or the Brookline Police at 617-730-2222 if you believe you've been the victim of a scam.

Please take the time to prevent scams and protect your financial security. Scams are prolific and ever-changing. All consumers need to be educated.

Ruthann Dobek, LICSW
Director

Miriam Rosalyn Diamond, PhD
Communications Specialist, Editor



ADDING LIFE TO THE YEARS
Brookline Senior Center

93 Winchester Street, Brookline, MA 02446

**Beth Israel Deaconess
Medical Center is proud
to support the Brookline
Senior Center. Thank you
for fostering a welcoming
community for seniors
to socialize, volunteer,
and stay active.**

Contents

Overview and How to Use This Resource	2	Financial Management	22
General Scam Information	5	Banks.....	22
Phone Calls.....	5	Bill Paying by Check.....	23
Emails	7	Charity Solicitations.....	23
Text Messages.....	7	Credit, Debit and SNAP Cards	24
Positive/“Good News” Scams	8	Data Breaches/Identity Theft.....	26
Celebrity Messages.....	8	Investments, Bitcoin and Other Cryptocurrencies, Loan Approvals.....	27
Letters From Santa	8	P2P Phone/Electronic Payments	28
Lotteries, Contests, Sweepstakes Winner	9	Government	29
Online Dating/Romance.....	9	EZDrive Electronic Toll Payment.....	29
Travel and Vacations.....	10	IRS/Tax Return.....	29
Consumer Scams (Buying and Selling Merchandise)	12	Jury Duty	30
Car Warranties	12	Medicare.....	31
E-Cards (Online Birthday and Greeting Cards).....	13	Natural Disaster Survivors	32
Florists.....	13	Police And Homeland Security	33
Genetic Screening/Testing	13	Postage Stamp Scams.....	33
Gift Cards	14	Social Security	34
Online Shopping	14	Unemployment.....	34
Package Delivery.....	15	Veteran And Military Family Scams	35
Selling Your Items Online.....	16	Home	36
Streaming TV and Movie Entertainment.....	17	Home Refinancing	36
Tickets For Shows and Sport Events.....	17	Home Repair, Improvement, Contractors.....	36
Scams Involving Family & Friends	18	Home Warranty.....	38
Bereavement and Obituaries	18	Homeowner Deeds.....	38
Clergy Messages	19	Trash with Personal Information	39
Facebook and Social Media	19	Utility Callers and Workers	39
Family/Friend Emergency.....	21	Technology	40
		Computer Virus, Malware Notification.....	40
		QR (Quick Response) Codes	41
		Wi-Fi Public Internet Access	41

Overview and How to Use This Resource

The purpose of this booklet is to empower you to take steps that can help protect personal data and assets, keeping them from falling into the wrong hands. It also provides guidance on actions to take when suspecting that you may have been scammed.

The reason for this publication

Unfortunately, there are con artists who try to access others' personal information for their own benefit. Often they are seeking to acquire money, although sometimes they have other motives. The United States Federal Trade Commission states that in 2023 consumers lost \$10 billion to fraudulent schemes and scams¹.

Defining scams

The Massachusetts *A Consumer Guide to Scams* defines a scam as “a dishonest attempt by an individual or organization to obtain something of value from you, such as personal information or money. Scammers may pose as legitimate organizations or government agencies (even your personal relatives and friends). Scam attempts can be made over the phone, in person, through letters, email, or by text message.”²

The AARP reports that most individuals are sent about 12 deceitful communications daily³. Connivers try to trick their prey into sharing identity details and/or funds. They may appear helpful and friendly (as in online dating scams) or threaten serious consequences to those who do not comply with their directions.

Kinds of information scammers want

Swindlers often seek data (such as Social Security, Medicare, or monetary account numbers) that enable them to impersonate someone so they can access or create financial records in that person's name (“identity theft”). They may try to fool people into revealing passwords so the scammers can access the accounts.

Schemers may also seek email addresses and phone numbers where they can send phony messages. They can look for biographical information, such as birth dates and places, schools attended, and mothers' maiden names so they can answer security questions when stealing identities. Or they may pose as legitimate officials and trick their prey into revealing further information

Others imitate real companies or create phony ones to charge for goods and services that they will not provide.

Examples of suspicious activity

- An organization or utility requesting or demanding immediate payment, often in gift cards.
- A notification from an agency stating that they need information such as your Social Security, credit card, Medicare, or bank account number and/or password.
- A message that appears to come from a friend, relative, clergy, merchant or association to which you belong asking you to click on a link or send money immediately.
- You seem to be losing money and don't know where it's going, or it appears to be spent in places and/or amounts you did not authorize.

¹Federal Trade Commission. “As Nationwide Fraud Losses Top \$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public,” February 9, 2024. <https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>

²<https://www.mass.gov/consumer-rights-and-resources>

³Schwartz, A. A. (May 2024) I Never Thought I Could be Scammed... Until I Was. *AARP Bulletin*. 26

- Your phone Caller ID or email source may look like it originated from a legitimate organization or individual you know, but may in fact not come from them.

Because there are many types of scams with new ones constantly emerging, it is impossible to compile a complete list. This publication highlights some currently prevalent schemes and ways to identify suspicious activity in general.

You can stay updated on new and emerging scams at the AARP's Fraud Watch Network <https://www.aarp.org/money/scams-fraud/fraud-watch-network/> . In addition, people may register to receive regular Watchdog Alerts via the website or by texting FWN to 50757 for text updates. The Federal Trade Commission also sends notifications regarding new schemes; registration is available at **FTC Consumer Alerts (govdelivery.com)** .

Steps to ensure that the person or organization you are dealing with is authentic

- *Pause. Do not give in to pressure to act, provide information, click, or respond immediately.* Many swindlers emphasize the need for immediate action and base their operations on consumer fear. By doing so, they aim to minimize the likelihood of their target detecting clues that something is irregular. Before making a commitment or sharing information, step back and consider investigating the situation further.
- *If you receive a call, email, or text you didn't initiate, do not furnish any personal data.* You may tell the person you will call or email them back, **look up and use the number or email of the organization or person that you have in your records** and verify whether the call or email is legitimate. **Do not redial the number or reply to the email that was used to contact you** (unless they match those on official documents and websites).
- Beware of people going door-to-door offering services or collecting information. When anyone (such as repair people) arrives at your home in person, ask for identification. A shirt, jacket, or nametag is not proof of someone's professional status. You can call the company they claim to represent using a number you already have (not one furnished by the individual) to verify their legitimacy.
- If you wonder about the authenticity of a request for payment or financial information, consult with your bank before acting about whether the situation sounds suspicious. Their staff are trained to spot warning signs of fraud.

Actions to take if you think you've been scammed

Don't be embarrassed about being in this situation. These frauds have become very sophisticated and are designed to trap intelligent people.

You don't have to deal with this alone! Confide in a trusted family member or ask a friend to assist you. The **Brookline Council of Aging Social Worker of the Day** (available at **617-730-2777**) can provide support and direction. Additionally, if you or someone you care for has fallen prey to multiple scams in a short period of time, Social Workers can discuss whether it might be appropriate to schedule a cognitive evaluation.

Call **9-1-1** immediately if you receive a message that a relative has been kidnapped, or that "police" are threatening to come to your house to arrest you if you don't comply with directions. For all other suspected scam or fraud cases, contact the **Brookline Police Department at 617-730-2222**.

Note what information the scammers may have accessed (such as Social Security, bank, or credit card numbers) and inform the firm where that account is housed that you feel you have been scammed. Notify any company whose gift cards you used as payment. Carefully monitor all financial (bank, retirement, credit card) statements and report any unauthorized charges to that organization.

Place a fraud alert with the credit reporting companies (one may be sufficient if they share with the others):

- Equifax.com
- Experian.com
- Transunion.com

Additional steps one can take

Call the **National Elder Fraud Hotline at 833-FRAUD-11 (833-372-8311)** Monday–Friday, 10:00 a.m.–6:00 p.m. Eastern Time. Case managers can offer resources and connect you with other appropriate agencies. They may help you submit a form to the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) at <https://www.ic3.gov/Home/ComplaintChoice> and/or a Federal Trade Commission consumer complaint at <https://reportfraud.ftc.gov/#/>

Contact the **Massachusetts Attorney General’s Office Consumer Hotline at 1-617-727-8400** to file a complaint about a scam or to check out a business. Complaints can also be registered online through the **Consumer Complaint form at <https://www.mass.gov/get-consumer-support>**. People ages 60 and older can reach a special Elder Hotline at **1-888-243-5337**.

The **Massachusetts Office of Consumer Affairs & Business Regulation Consumer Hotline** can be reached at **1-888-283-3757**

Any senior can reach out to the **AARP Fraud Watch Network Helpline** (regardless of AARP membership) at **877-908-3360** Monday through Friday, 8 a.m. to 8 p.m. ET. Staff offer information and direction on steps to take.

You can also get support for dealing with the stress and emotional aspects of this situation at aarp.org/FraudSupport

How to use this publication

There are a few ways you can benefit from the information provided here.

First, this book can be utilized as a reference for looking up specific situations you are facing and wonder whether they may involve fraud. If the condition is listed, you may follow the steps provided.

Please note: The information provided here is limited and scams constantly change. Readers facing specific incidents that are not included or that vary from the details provided are encouraged to consult with the **Brookline Council of Aging Social Worker of the Day at 617-730-2777** and/or the **AARP Fraud Watch Network Helpline at 877-908-3360** to determine how to respond.

Second, readers can peruse this booklet to become aware of and alert to the range of common current scams. This can increase their ability to identify and deal with many questionable circumstances before they arise.

Finally, this publication may be used as a guide for protective measures that can be taken at any time to lessen the possibility of future threats. Most topics include a “Prevention” list that allows readers to be proactive in increasing the safety of their identity and belongings.

Most important, this book provides reassurance that you do not have to face these challenges alone and identifies many free resources for guidance and support.

Sources:

AARP Fraud Resource Center <https://www.aarp.org/membership/benefits/finance/fraud-resource-center/>

Commonwealth of Massachusetts (2023) A Consumer Guide to Scams <https://www.mass.gov/guides/a-consumer-guide-to-scams>

Federal Trade Commission

JVS of Metrowest

The Massachusetts State Attorney General’s Office

Pension Action Center

US Federal Bureau of Investigations

General Scam Information

Watch Out For Phone Calls

Description

Phone scammers often try to convince people to buy a product, service or donate to a charity. They may also attempt to persuade you to reveal personal information, such as credit card or Social Security numbers. Alternatively, they may say that you owe money and must pay immediately, often by purchasing gift cards.

Another ruse is calling and hanging up after the phone rings once, hoping recipients will return the call without knowing they will be charged an international rate for calling back.

In a related scam, the caller says they dialed the wrong number, and then tries to entice the individual to invest in a “great opportunity.”

Some scammers use **Caller ID Spoofing**. This is when the number on a phone’s caller ID falsely appears as though it comes from a specific company (such as bank, government department, utility, or charity). It may also seem to be from a specific person. The caller may know your personal information (your address, birthdate, mother’s maiden name, name of high school, where you grew up), which makes it sound like they are the actual company and know the answers to your security questions. This misleads people to pick up calls they may and provide personal or financial information.

Some scammers record an individual saying “Yes.” They may ask “Can you hear me?” or “Is this _____ (your name)?” The recording of “Yes” is then spliced onto a different question (such as “Do you agree to pay for”) as “proof” that the person approved charges for something they did not.

In a related ploy, callers take a recording of the person’s voice and create a “deepfake” rendition saying whatever the schemers choose. For instance, a imitated voice could be used to contact financial institutions that have voice recognition software and instruct them to withdraw or transfer personal funds.

Spot the Scam

- The phone stops ringing after one ring.
- There is an unnaturally long pause after you pick up the call.
- A recorded voice says to press a number to “opt-out.”
- The caller states that you are eligible for an amazing financial investment, a special deal, a prize, or have won the lottery.
- The person on the other end pressures you, such as saying that you must make up your mind immediately or the offer expires.
- The caller insists on payment for a late bill, missed jury duty, etc., and threatens that you will be arrested, turned over to a Collections company, or that utilities will be shut off if not paid immediately.
- You hear a robotic voice and/or background noise on the call.
- The person asks a Yes/No question such as “Can you hear me?”

Stop the Scam

During a Call

- If you pick up a call and are concerned that it is a scam, hang-up immediately.
- Do not press any numbers on your phone during the call, even if the caller/message indicates that this will ensure that you will no longer receive these calls.
- Do not reply to questions, especially if your answer is “yes.”
- Do not give into pressure to make decisions or payments on the spot.
- Do not give out your credit card, bank, or personal information during unexpected incoming phone calls.
- Do not pay companies with gift cards.
- If you are concerned that the caller represents an actual business or government department, hang up and call the phone number listed on the firm’s legitimate website to verify the information provided.

After a Suspicious Call

- Make a point to regularly review your phone bill for questionable or unexpected call charges. Notify your phone company immediately if you see a charge that looks inaccurate.
- If you are concerned about a call Robocall you received, particularly if you’re on the Do Not Call registry, report it to **www.donotcall.gov** and to the FCC at **www.fcc.gov/complaints**

Prevention

- Do not pick up calls from unknown or unexpected numbers. If a call is important, the caller will leave a message.
- Sign up for both the state and national “Do Not Call” registries to limit telemarketers’ ability to reach you. (Please note doing so will not prevent all scam calls, and you still need to remain vigilant.) You can enroll in the Massachusetts registry at: **https://www.mass.gov/massachusetts-do-not-call-list** The U.S. Federal registry is available at: **https://www.donotcall.gov/register.html#step1**
- If you never make or receive international calls, ask your phone company about blocking calls from other countries. This will prevent anyone using your phone line from returning a call that is actually from outside the U.S. without realizing it.
- If your phone rings once, then stops before you answer it, do not return the call.
- Turn off “Air Drop,” “Name drop,” or “Devices Together” cell phone apps when you are not actively using them.
- Keep a list of verified phone numbers (culled from actual documents) that you can call directly if necessary. These can include your bank, utilities, police and any other business with which you interact. (Do not assume that an incoming call that appears to originate from one of these numbers is legitimate, however.)
- Set up a password for accessing your voicemail, even when you call from your own phone.
- Opt-out of voice recognition access to accounts, such as banks and investment companies.
- Use the default automated answer as your phone greeting. Do not record your own message or name.
- Add the phone numbers of everyone who may call you to your phone’s contact list, from friends and family to your bank and doctor. Then, if your phone allows, select the option to “silence unknown callers.” That will send their calls directly to voicemail for you to review later and evaluate if they seem legitimate.

Emails

Description of the Scam

Scammers send messages (and hard copy letters) that falsely appear to come from a well-known business, but contain misinformation directing recipients to contact them using links, email addresses, or phone numbers that will connect them with bad actors looking for money or personal information.

Spot the Scam

Although emails may appear to come from individuals and businesses you know - and may even contain familiar logos and fonts - the senders' email address itself may appear strange. There may also be misspellings and typos in the subject and content of the message.

Stop the Scam

Don't open email originating from a strange sender address, even if it's from a person or company that seems legitimate. If you do open it by mistake, do not click on any links provided and delete it immediately. Beware of messages directing you to sites like **anydesk.com**

Prevention

Regularly delete all email in your Spam/Junk and Trash folders.

Text Messages

Description of the Scams

Recipients get an unexpected text (SMS) message that may appear to come from a familiar company, bank, or US agency in an attempt to trick people into providing account numbers and other confidential information. (This is also referred to as "smishing.")

Or they may receive messages that seem to have been sent to the wrong number by mistake. When the person replies that it's the wrong number, the wrongdoers can commit fraud.

Sometimes packages arrive for individuals that did not order them (are not gifts). They then get charged for the items.

Spot the Scam

Messages may claim that "your account has been suspended", "there is suspicious activity on your account", "there is a problem with your shipping address" or "there is a package waiting for you."

There may also be typos or misspellings in the message.

Stop the Scam

Do not reply to unexpected text messages from unknown senders. Delete the message and block the number.

Locate the company's verified email or phone number via a legitimate website and contact them to check the veracity of the message.

Do not pay for items that you did not order. You can mark the unopened package "Return to Sender." Or if you do open it and choose to keep the item, know that you are legally not required to pay for something you did not order.

POSITIVE/"GOOD NEWS" SCAMS

Celebrity Messages

Description of the Scam

People receive messages, concert invitations, and merchandise endorsements that falsely appear to come from celebrities. Using Artificial Intelligence, these communications may even come across as live phone or video calls or messages. The "celebrity" then asks for fan information, money/loans, or other assistance.

Stop the Scam

Be wary of any direct contact that appears to come from someone famous whom you do not personally know.

Do not provide funds or data about yourself.

Do not make purchases based on "celebrity" endorsements.

Letters from Santa

Description of the Scam

Thieves may pose as companies offering Christmas letters "from Santa Claus" to send to children as a surprise. They may have several motives, from stealing consumer money without providing letters, to acquiring credit card numbers for their own use. They may even gather information on children receiving the letters to set up false accounts in the child's name and then spend money which will ultimately be charged to the child.

Spot the Scam

You may receive an unsolicited message from a company offering to send personalized Santa Claus letters to children for free or for a nominal fee.

Stop the Scam

Do not click on links or respond to these messages.

If You Have Ordered Letters

Monitor your credit card account to ensure that all posted charges are legitimate.

Check the child's credit rating on a regular basis (at [Equifax.com](https://www.equifax.com), [Experian.com](https://www.experian.com) and or [Transunion.com](https://www.transunion.com)) to ensure that there are no false accounts established in their name.

If you spot anything erroneous or suspicious, immediately contact the Police at 9-1-1.

Prevention

Write your own personal letters "from Santa" (or ask a friend to write them if you're concerned that your handwriting will be recognized). You also create a certificate using a computer stating that the children are on the "nice list."

Lotteries, Contests, Sweepstakes Winner

Description

What appears to be online contests may actually be merchants or scammers trying to get your personal information.

In another scheme, individuals receive notification that they won the lottery - either in the US or abroad. They are told that they are required to pay a processing fee or taxes before they can receive the money. Or that they must provide their bank account and social security numbers in order to receive their winnings. Another variation is directing “winners” to open a new bank account where prize can be sent.

Once the scoundrels have the account information, they may initially make small checks or withdrawals to see if it gets noticed. If this goes undetected, they will move onto taking larger amounts.

After a big lottery win fake announcements may be made on social media sites stating that the winner will provide cash to anyone sharing or retweeting a post.

Spot the Scam

If you are told you won a lottery, it is a scam. When people win lotteries, they are not notified; they need to identify themselves as the winners to the commission running the lottery.

Prize winners do not have to pay upfront, provide information, or open special accounts to receive prizes.

If you don't recall entering the sweepstakes, this is a scam. You can't win a contest that you didn't enter.

Do not believe anyone saying you won or have a good chance of winning a lottery outside the US by paying over the phone or mail. One cannot legally enter an international lottery by phone or mail.

Stop the Scam

Do not provide any money or bank information. Do not open a new account.

If you feel someone is trying to scam you with a lottery hoax, contact one of the following:

- Call the Brookline Police at **617-730-2222**.
- The Federal Trade Commission at **ReportFraud.ftc.gov** or **877-382-4357**.
- The State Attorney General's Office at 617-727-8400 or the Elder Hotline at **1-888-243-5337**.
- The Massachusetts Office of Consumer Affairs and Business Regulation at **617-973-8787** or **888-283-3757**.

Online Dating/Romance

Description of the Scam

People posting on social media, online dating apps and websites looking for romance might be scammers posing as someone else in an attempt to get money and/or their victim's personal details that they can use for personal gain.

They may also request explicit pictures and then blackmail their victim, threatening to post or share the photos publicly unless paid off.

Spot the Scam

Check if the name matches photos of the same person on other websites. Right-click the photo, choose “Copy Image Link” (or “Address”). On Google's search site, click on the camera icon to the left of the text search bar, paste the link, then click “find image source.” Go to any websites listed to see the name associated with the photo.

Often the relationship seems to get very close very quickly, including messaging, emails, and/or chat.

After starting what appears to be a loving relationship, the individual may say that they need money. They may state that they have to pay for medical expenses or were robbed.

The person may offer an excuse for never being able to meet in person, such as they live or work (sometimes “temporarily”) too far away.

Alternatively, they may indicate that they want to visit you and need funds to pay for the trip. Similarly, they could claim that they are sending you a gift and need money to ship it or pay customs fees. They may also ask you to put their name on a bank account or open a new one.

They might also offer to help you make money by sharing business and/or real estate investment leads.

They usually ask for funds to be sent using gift cards, cryptocurrency, or wire.

Any requests for money are red flags.

They may also encourage you to send explicit pictures of yourself.

Stop the Scam

If, after following the above steps, you find the person’s name does not match that listed elsewhere on the internet for the same or similar photo, block that person from contacting you and report them to the website administrators.

Do not send money, photos, or personal information. Do not invest where they suggest or provide access to accounts.

Consult with a trusted friend or professional if you’re unsure whether the person seems genuine.

If You Suspect You are Being Scammed

Notify the website where you met the person about suspicious individuals.

Contact the Federal Trade Commission at <https://reportfraud.ftc.gov/#/>

If you’re concerned about being blackmailed, contact the FBI at <https://www.ic3.gov/Home/FileComplaint>

Prevention

Don’t provide money, intimate photos or personal financial details early in a relationship or to someone you haven’t met in person.

Travel and Vacation Scams

Description of the Scams

Websites that seem to belong to familiar brand name companies might be bogus imitations. These may show up in searches for hotels, tours, rental vacation properties, and other amenities. Although they look official, and even may have the company’s name in their URL, they are set up to steal consumers’ money and/or credit card information without providing the services promised. If posing as airlines, they may steal individuals’ identity from TSA information provided.

Scammers also send emails offering “free” trips to trick people into sharing credit card numbers and/or clicking on links that infect computers.

People posing as insurance agents may offer fake trip cancellation policies.

Another scam occurs to people staying in legitimate hotels. They can get calls in their rooms falsely claiming to be from staff stating that there's a problem with the credit card used for the reservation or at check-in. They will ask for the number again or for another card number. (These calls are often placed early in the morning or very late, when the guest is less likely to go to the front desk in person.)

Spot the Scams

Be suspicious of bargains that appear unbelievably good. Always be wary of renters and/or companies that do not accept credit cards, and instead request payment via money wire, cash, or gift cards.

Check the spelling and grammar of the URL or at the website. If you spot errors, it may be a sham site.

Be wary of websites claiming to accelerate travel visas for an extra fee.

Stop the Scams

Do not click on links in emails offering free or very inexpensive flights, or warnings that hotel or airline frequent flyer miles will soon lapse.

For vacation rentals, check out the property to confirm that it's a legitimate place. You can turn to <https://maps.google.com/> to investigate whether the location corresponds to the description. Look up the renter/homeowner by name to ensure that it's the same name on the lease.

Be extra cautious when making reservations on third-party websites. Check them out with the Better Business Bureau at <https://www.bbb.org/> before paying, in addition to searching reviews of the company.

After booking a hotel, flight and/or tour, contact the company directly to confirm your reservation. If they don't have it, immediately notify your credit card company and reach out to the National Elder Fraud Hotline at **833-FRAUD-11 (833-372-8311)** for assistance. You may also file a report with the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) at <https://www.ic3.gov/Home/ComplaintChoice> and/or the Federal Trade Commission at <https://reportfraud.ftc.gov/#/>

Go to the front desk in person if, after check-in, you receive a call or message that there's a problem or need to confirm the credit card used for the reservation. Do not confirm or give out a credit card number remotely.

Prevention

Make hotel reservations through the property's official website or app.

Pay with credit cards. Do not send cash or gift cards or wire funds.

Get a purchase and/or rental agreement in writing. It's a good idea to ask someone you trust to review all agreements and cancellation policies before you pay. Make sure you understand penalties and restrictions related to the transaction.

Go directly to <https://www.tsa.gov/precheck> if you want to enroll in the TSA PreCheck program.

If you need a tourist visa to visit another country, find the country's correct link at travel.state.gov.

Consumer Scams

(Buying And Selling Merchandise)

Car Warranties

Description of the Scam

People get phone calls and messages - typically recorded - or letters in the mail from companies incorrectly stating that their manufacturer's automobile warranty is about to expire and needs to be updated. This is a scam to get money and/or financial details without providing coverage.

Spot the Scam

Offers for updated warranties are almost always rackets.

If you've signed up for the Do Not Call Registry and get an unexpected call like this, it is almost certainly a scam.

The notification may stress the necessity for immediate action.

The communication may dishonestly state that they are affiliated with the car manufacturer. Mailings may look deceptively official.

If you accidentally press a button during a phone call, a live person may answer who has accurate information on your automobile. (These facts are actually publicly available.)

Stop the Scam

Don't pick up phone calls from unfamiliar numbers.

If you happen to answer and get a message about your car warranty, hang up and don't push any buttons or provide information.

Verify for yourself the actual expiration date on your warranty paperwork, as well as information on ways to extend it. (Do not share this information.)

If the caller says they are from the dealer where you purchased your car, end the call and locate the dealer's phone number on your sales receipts or from a reputable website such as the Better Business Bureau (www.bbb.org). Call the dealer directly to verify the notification you received.

Do not do business with any company unless it's verified by a reputable source such as the Better Business Bureau (www.bbb.org).

Before signing and/or providing any payments, carefully read contracts - and ask someone else to assist you - to determine what is covered and the duration of the agreement.

You can also inform one or more of the following about the notification you received so they can track and clamp down on fake businesses:

- Federal Trade Commission at <https://reportfraud.ftc.gov/>
- Federal Communications Commission at <https://consumercomplaints.fcc.gov/hc/en-us>
- Massachusetts State Attorney General's office <https://www.mass.gov/how-to/file-a-consumer-complaint>
- Better Business Bureau <https://www.bbb.org/file-a-complaint>

Prevention

Make sure you're enrolled in the National Do Not Call Registry. <https://www.donotcall.gov/register.html#step1>

Block calls from this number on both cell and landline phones.

If you want to purchase a new warranty, ask your automobile manufacturer or the American Automobile Association (AAA) for referrals.

E-Cards/Online Birthday and Greeting Cards

Description of the Scam

What appears to be an online greeting card may actually contain malware that can harm devices or access private data and put the sender or viewer at risk of identity theft.

Spot the Scam

E-Card notifications may or may not specify the name of the sender. In some cases, the notices state that the card was sent by an “admirer.”

Stop the Scam

Do not open links to cards if you are unsure who sent them.

If you know the “sender”, contact that individual directly to confirm that the message did in fact come from them before clicking the link.

Florists

Description of the Scam

There are schemes where businesses claiming to be florists offer impressive deals in order to get money and/or credit card information. They may appear in online searches, send out notifications, or post ads online. They can be particularly active during key holidays, such as Valentines and Mothers’ Days.

Stop the Scam

Do not click on email links.

Prevention

As with all businesses, research florists (via sites such as the Better Business Bureau) before placing an online order.

Genetic Screening/Testing

Description of the Scam

A stranger offers genetic screening they say will determine personal risk for medical conditions. They may reach out by phone, mail, in person, or at health fairs. Tests such as cheek swabs may be offered or provided.

Their aim may be to charge Medicare for unnecessary services. Or they may gather individual Medicare numbers to run up a host of false charges.

If Medicare is billed for a test that was not authorized by the individual’s approved physician, the claim may be denied. The individual may then be held responsible for the test in full, which could cost over a thousand dollars.

Spot the Scam

You receive an offer of no-cost medical genetic testing, as long as you provide your Medicare number. Or a packet you were not expecting arrives in the mail.

Stop the Scam

Do not use or reply to a genetic test packet that your doctor did not order. Return the package while keeping a record of the vendor’s name and the date you mailed it back.

Prevention

Always consult your physician prior to enrolling or participating in medical genetic testing.

Gift Cards

Description of the Scam

Crooks open unpurchased card envelopes in stores, steal the information, replace the cards, and place their own charges once cards are bought and activated.

Alternatively, swindlers on bidding websites may sell cards that are counterfeit, expired, or used.

Scammers may also send messages that falsely appear to come from familiar colleagues encouraging the purchase of gift cards as a surprise for someone you both know.

When reputable businesses close, bad actors sometimes buy the company's old phone number, and create a voice message falsely stating that people thinking they are calling the former business have won a gift card and need to leave personal information to redeem it.

Spot the Scam

The packaging of gift cards sold in stores may not be intact and/or the cover of the PIN may have been removed.

Stop the Scam

Do not buy resold gift cards.

In stores, do not buy gift cards that appear in even slightly ripped or open packaging, especially if the PIN is exposed.

Do not reply or agree to requests of buying gift cards for an acquaintance without verifying the message's authenticity. Contact the sender directly through a new message using the email address or phone number you have from previous interactions.

Hang up if you call a company that you have done business with in the past and reach a recording stating that you won a gift card.

Prevention

Only redeem cards with the company that provided them.

Online Shopping

Description of the Scams

Some consumer websites that appear to belong to reputable companies (such as Amazon) are actually imitations set up by culprits seeking credit card information.

In addition, thieves access data provided by individuals - even on verifiable websites - over public/shared wi-fi services.

Culprits also send emails that appear to come from well-known businesses stating that there is a problem with your account or that suspicious activity has occurred with a link to click to remedy the matter. The link leads to a bogus website established to steal details and/or money.

A notification from an online business you use may state that you owe them money (often indicated as "payment declined"), or that they owe you money.

Another scam is merchandise that appears to be for sale at a fraction of its usual price, which is actually a hoax to get money and/or credit card information.

Ads from fake companies are not screened by social media companies and may appear legitimate.

Stop the Scams

Scrutinize website URLs to ensure you're ordering from the correct seller and not an imitation. Do not click on links in unexpected emails.

Investigate sellers prior to making purchases, even if the website appears official. Check them out with the Better Business Bureau at <https://www.bbb.org/>, or type in the company name and the word “reviews” to view comments from other purchasers.

Do not click ads that pop-up or links in emails.

Type in the correct url for the company using legitimate information and contact them using their official customer service.

Don't provide information to companies that contact you. If it's a phone call, tell them you'll call back and hang up. Do not call the number that was provided by the caller or listed on caller ID unless it matches the official one you have.

Research merchandise sales and be wary of buying something that appears to be a tremendous bargain unless you can confidently validate the seller.

Prevention

Use a private, protected internet connection (not a public shared one) when purchasing items online. Only submit your credit card number on websites that begin with “https://”

Make purchases using credit cards only. (This is the most secure method.)

Package Delivery

Description of the Scam

Emails, text messages and phone calls may appear to come from the US Postal Service, a delivery company (such as UPS or FedEx), or a package driver who is unable to find your home. If you aren't expecting a package, they might state that they have a gift. They may request your credit card number (in some cases stating that you need to pay an alcohol delivery fee). Or they could leave a notice at your door indicating requesting a call to make a delivery. Their aim is to get your personal information, money, or to have you click on a link that will infect your computer.

Spot the Scam

You receive a message regarding a package you aren't expecting.

You may be told to pay or disclose private or financial data in order to accept delivery.

The message could come from an email with an actual address that doesn't exactly match that of the shipping company when you independently type in the company's website (without clicking on any links in the email).

Stop the Scam

Keep a record of merchandise ordered and track its delivery status and timing.

Be particularly cautious about notifications of deliveries that you are not expecting. Do not click on links, provide or confirm information or in response to an email for a delivery you are not expecting.

Contact the presumed seller or delivery company directly using the correct number or email address on their actual website (not one provided in the message) to verify the information before taking any action, including clicking on links.

When you get an email about a package, hover your cursor pointer above any links provided before clicking to see if the website URL is correct.

Never give your credit card number or password to someone who contacts you.

Don't call phone numbers listed on a missed-delivery notice. If the company is one with which you're familiar, look up the actual number of the company and call them directly to confirm that the notice is legitimate.

Be aware that there is no alcohol delivery fee.

Don't accept “gifts” that seem suspicious.

For Suspected Delivery Scams

Contact the Federal Trade Commission, at <https://reportfraud.ftc.gov/#/> or **877-382-4357**.

Emails and other online scams can be reported to the FBI's Internet Crime Complaint Center <https://www.ic3.gov/>

Forward suspicious emails and the following delivery services of concerning messages, and/or fake-looking websites, then delete them:

- UPS - **fraud@ups.com**
- FedEx - **abuse@fedex.com**
- U.S. Postal Service - **spam@uspis.gov**

Report fraudulent-looking text messages claiming to be from the U.S. Postal Service. Information is available at: <https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams>

Prevention

You can register for the US Postal Service's notification program at informedelivery.usps.com This service emails recipients electronically scanned photos of letters and packages 1-2 days before delivery.

When ordering items that may arrive when you might not be home, try to have them sent to an office where you or someone you know can receive them in person. If that is not feasible, request that neighbors retrieve them when you are not available. Or consider having them delivered to a nearby package delivery locker (often available through the U.S. Postal Service and Amazon).

Selling Your Items Online

Description of the Scam

Scammers pose as people purchasing items with the aim of conning sellers out of money.

Spot the Scams

There are several variations to this.

The "buyer" may send a payment, often as a check, that's above the agreed upon item cost amount. They ask you to send them the difference when you mail out the item. In actuality, the payment they sent you was false (although it may initially appear as a credit in your account) and they will keep the money you give them as "change."

The "purchaser" says they will pay via a mobile payment app. The notification you receive that the money has been sent is actually fake, and the scammer hopes you will send the item even though they have not actually paid for it.

The "buyer" says they want to confirm who you are before purchasing the item. They send a text message with a Google Voice verification code, and ask you to give them the code. This is a ploy to create a Google Voice account connected with your telephone number and use it to cheat other sellers under your phone number and identity.

Stop the Scam

When possible, only sell items to people who live near you and can pay in cash in person.

Only accept mobile payments from people you know personally and trust.

Do not accept a check that is above the price of the item(s) sold.

Do not share verification codes sent to you (via phone, email, or text) with someone you don't know.

Streaming TV and Movie Entertainment

Description of the Scam

Consumers get bogus notifications or calls stating that their Netflix, Amazon or other streaming account will be terminated unless they are promptly paid. When the individual replies or clicks on links, they may get robbed.

Spot the Scam

The message may appear legitimate, including logos, etc.

When you hover over the sender's email address, it may or may not match that of the company.

Stop the Scam

Do not reply, click on provided links, or call the phone number listed.

Independently locate the business' actual website and validate the status of your account with them.

Tickets for shows and sport events

Description of the Scam

Tickets - especially for shows that are in high demand - are offered on social media, fake websites made to look official, and platforms such as Craigslist. Once they get the money, the scammers might send counterfeit tickets or nothing at all.

Even genuine websites, like Ticketmaster, may have malware embedded in purchase forms, which may expose credit card information to crooks.

Spot the Scam

Sham ticket sellers may ask for payment via platforms such as Zelle or Venmo, as opposed to credit cards.

Stop the Scam

Make sure you're buying tickets from a reputable agency, such as the real Ticketmaster or StubHub by double checking the URL and confirming that you're on the actual website. You can verify the company selling the tickets through the National Association of Ticket Brokers (NATB) at natb.org or at verifiedticketsource.com

Before paying for a ticket, check the online floor seating chart on the venue's genuine website to verify that the seat that you are purchasing exists.

Do not wire money or pay someone you don't know through apps such as Zelle, Venmo, PayPal, or CashApp.

Prevention

Be wary of agencies selling tickets to an event that is in high demand.

When buying from private individuals (as opposed to companies), only purchase from people you've met.

Make sure you have an antivirus program installed on your device.

People using Apple Pay can hide their credit card information.

If you suspect you have been scammed

Notify the Brookline Police at **617-730-2222**.

Inform the Federal Trade Commission at ReportFraud.ftc.gov or **877-382-4357**.

Contact the FBI Internet Crime Complaint Center at IC3.gov

Scams Involving Family & Friends

Bereavement and Obituaries

Description of the Scams

Scammers glean personal information from obituaries and publicly available death certificates to commit identity theft on mourners.

One ruse is taking over the deceased person's cell phone number (without having the actual phone) by convincing the carrier that they are relatives and asking to transfer the old number to another phone. They can then access authentication numbers needed to use and/or set up accounts in the name of the person who died.

Thieves also use this information to anticipate when homes will likely be unattended (such as during a funeral or wake) and could be robbed.

Spot the Scams

Financial accounts list charges made after individual's passing.

The person's cell phone suddenly stops working before the survivors close down the account.

Stop the Scams

Call the Brookline Police at **617-730-2222** to report suspicious activity and theft.

Tell the cell phone service provider to immediately close down the number.

Notify banks and credit card companies of fraudulent charges.

Close the individual's email account(s).

Prevention

Soon after a person dies and prior to posting online obituaries, terminate their cell phone number and service. Also inform banks, credit cards and agencies, as well as email providers.

When creating obituaries, list few - if any - details (such as maiden names and birth places) that can compromise the security of survivors' identities.

Provide as little information as possible in public notices regarding the timing of services.

Refrain from listing unnecessary details on the locations of relatives' current residences.

Plan ahead by checking if your own cell phone carrier offers the opportunity to designate a "legacy contact" person who will have sole access to the line after your own passing. Create a list of all your email providers as well as online financial accounts and apps with sign-in information and inform your legacy contact where they can locate this document after your demise. This will enable them to monitor and secure these accounts.

Clergy Messages

Description of the Scam

Congregants receive a call, email or other message requesting donations. The communication appears to come from a religious leader, often someone they know from their own faith community. These can be thieves posing as clergy.

Spot the Scam

Be wary, especially if the email address used does not match previous authentic emails or what is listed on your congregation's website (even if the name appears to be correct).

Stop the Scam

Do not reply to the message. Write or call clergy at the email or phone number on your congregation's website to confirm whether the message was genuine. The safest way to donate is via credit card.

Facebook and Social Media

Description of the Scam

Scammers send invitations to connect over Facebook, LinkedIn, and other social media platforms. These requests may not be from who they purport to be. Sometimes they falsely appear to originate from individuals you know.

They may offer jobs, detailing specific start dates and salaries (sometimes including "payment" prior to the completion of any work).

Or they may appear as potential romantic partners (also see the entry about Online Dating).

There are predators seeking information, money, or to commit other crimes.

Some fraudsters threaten to release false pornographic photos or videos they created using innocent pictures shared online and then try to blackmail their victims.

Spot the Scam

Warning signs include invitations to connect with compliments (comments such as "You're so pretty").

Alternatively, the notifications may appear to be from a friend with whom you are already connected on that platform.

If you view the individual's profile, you may see minimal or inconsistent information. There may be very few original postings and comments on other people's posts (mostly "likes" or simply reposting other peoples' comments). The account may not have a photo or their full name may not be listed. Be suspicious about newly created accounts by people you do not know, or ones that haven't been updated in the past year. (On LinkedIn profiles, under "More" you can click on "About this Profile" to view details.)

If you are looking to network professionally, as on LinkedIn, and the person appears to be in your target field, look up the individual online and see if the social media profile matches their photo, job, and experience listed elsewhere.

You can check whether the person's name and photo are consistent with those listed on other websites. Copy a profile photo link by right-clicking on it. Go to a Google search page and click on the camera icon to the left of the search bar. Paste in the link, check "find image source," go to any websites that appear and identify whether the picture matches the name and information listed on social media. (Some platforms, such as LinkedIn, allow people to "Search Image with Google" directly by right-clicking on the photo.)

Stop the Scam

Do not accept invitations to connect with people you don't know or are unfamiliar with.

Do not click on any options or buttons provided in a message, even to indicate that you're uninterested in training programs or to discuss job opportunities.

If the source appears to be someone you know and are not already connected with on that platform, contact the person directly via email or phone to verify whether the notice is genuine.

If you search the person's photo and find it connected to a name that differs from that on the social media site, or if someone you know states that this is not their page, go to the suspicious person's profile page to block them from contacting you and report them to the social media administration.

If Your Own Account Has Been Hacked or Duplicated/Faked

Report the infraction to the social media administration.

If the account was hacked (accessed by someone else), close the account and open a new one, using a different password and photo. Alert your connections so they don't respond to false messages appearing under your name.

If you're being blackmailed, contact the FBI at <https://www.ic3.gov/Home/FileComplaint>

Prevention

Ensure that information on your social media accounts is as private as possible. To do so, go to the Settings page and click on the Privacy section to select options that minimize who can view your site and contact you. (For assistance with this, you can make an appointment with computer help experts at the Senior Center by calling **617-730-2777**).

You can set up two-step login authorization to reduce the likelihood that your account will be accessed by someone else.

Periodically search your own name and photo online to see if anything arises that you did not post or originate. If you find an account that is not authentically yours, immediately report it to the website administration and request that it be removed.

Family/Friend Emergency

Description of the Scam

Scammers call or send fake messages stating that a family member or friend is dealing with an emergency and desperately needs money to be freed and/or acquitted. The messages may appear to come directly from the friend or relative, and include some accurate details about them.

Using DeepFake technology, the caller may sound like the individual - or look like them if it's a video call. If it doesn't sound exactly like them, they may state that the phone connection is bad, or that their nose was broken in a tussle. The message may falsely indicate that the person was in an accident, was arrested, mugged, kidnapped, or in some other trouble and needs help.

Often these calls and messages arrive in the middle of the night, when the recipient may be tired and less likely to think clearly.

In reality, the individual is fine, and this is a ploy for the scammer to get money.

Spot the Scam

The caller may ask not to share the details of the arrest or difficulty with anyone. This is a red flag.

The person may tell the call recipient to contact specific "defense lawyers" and provide a "case number" to make the situation sound authentic.

Sometimes callers send messengers directly to the recipient's home to personally fetch the requested funds to get the relative released. They may even offer to drive the individual to the bank or ATM so cash can be withdrawn and immediately handed to the driver.

Stop the Scam

Do not provide payment in any form.

Do not phone any number provided by the caller, even if they claim it's a defense attorney.

Tell the caller you need to call them back, and ask for their phone number. Report the situation and number to 9-1-1 immediately.

After you hang up, try contacting the family member yourself on the phone number/email you already have. If they answer, check that they're fine. If they don't pick up or reply in a reasonable amount of time, notify another family member of the notification you received.

If it's an email, check the address from which the message was sent to see if it matches that of your friend/relative. Contact your friend/relative using previous email addresses or their actual phone number to confirm whether this indeed came from them.

Prevention

In advance of any emergency, create an agreed upon, not obvious, family password (such as a random object rather than a name) to use to check if a message is legitimate.

Refrain from sending funds when you feel panicked. Whenever you choose to send money (such as a birthday gift) to a friend or relative, verify their contact information and method of delivery in advance directly with them. Only send what you can afford. Check with them immediately to confirm that they received it.

FINANCIAL MANAGEMENT

Banking

Description of the Scams

Culprits use identity theft to access or take over bank accounts.

People may receive false notifications that appear to come from their bank, such as false scam alerts.

Spot the Scam

Check your credit through Equifax, Experian, and TransUnion every few months. Report any loan, account, or credit card listed that is not yours.

Regularly monitor your financial statements and notify your bank immediately if you see any unexpected charges or activity, including transactions of \$1 or less. (Some thieves initially attempt small charges as a test before making larger withdrawals.)

Stop the Scam

Notify your financial institution right away of any false charges. Banks are mandated to reimburse for fraudulent transactions if notified in a timely manner. (You may be responsible for a \$50 - 500 deduction, depending on how quickly it is reported).

Do not reply or click on links or call phone numbers in emails or text messages from banks. Instead, reach out to the bank using the number on your card regarding the veracity of the email.

Don't tell anyone your account numbers, security codes, PINs or passwords.

Do not click on unexpected links in emails, even if you know the sender.

Do not provide personal information, such as your birthdate, account numbers, or mother's maiden name to someone who contacts you, even if they sound legitimate. You can call them back at the business number you already have.

Inform the Brookline Police of thefts at **617-730-2222**.

Reach out to the Federal Trade Commission and FBI at **reportfraud.ftc.gov** and **IC3.gov**

Prevention

Use an online account username that is not your email address or something easy to guess.

Use a different password for each online and financial account. Avoid passwords such as "123456," "password," or family names that are easy to guess. Long passwords with numbers and symbols are best.

Establish multifactor authentication to sign into accounts, such as phone calls or text messages. Do not use voice or face recognition, as these can be spoofed.

Log out of banking and payment apps after each use.

Sign up to have your bank notify you immediately of any charges made with your credit and/or debit card.

Use online banking and frequently check your accounts for unauthorized activity.

Do not take online quizzes or surveys that ask for personal information such as your mother's maiden name or the year you completed high school. Do not post such information on social media.

If your bank allows, establish a (nonsense, difficult to guess) password and/or security questions for in-person transactions. Some banks also encourage customers to designate a trusted contact person that the institution can check with when they have concerns about activity.

Bill Paying by Check

Description of the Fraud

Thieves retrieve others' outgoing mail looking for checks. They "wash" out the recipient's name and amount, fill in their own names or businesses and often a larger amount of money, then cash or deposit the new amount in their own accounts.

Or they take a photo of the check and change it digitally to make it appear that it was made out to them.

They get access to the payments by robbing postal carriers of keys to home and USPS mailboxes. They may also pull mail from mailboxes, or take envelopes intended for pick up out of private mailboxes.

Once they have check information, they may use routing numbers to open new accounts, borrow money and/or establish credit lines in the account holder's name.

Stop the Fraud

Check your bank account and statements regularly. If you see a check listed that you did not write, notify the institution immediately. The institution needs to be informed within 30 days of the statement to replace stolen money.

If a check you wrote was not posted or cashed in the usual time frame, contact your bank to stop payment.

Inform the Postal Inspection Service, as well as all 3 credit reporting companies:

- Equifax.com
- Experian.com
- Transunion.com

Prevention

Remit payments electronically using a private internet connection

If writing checks, use a permanent black or blue gel ink pen, which is harder to wash out.

Mail envelopes with checks included inside a post office. If possible, hand them directly to a clerk.

If you are unable to do either of the above and must put envelopes in a public mailbox, do so close to the last scheduled pickup time.

Remove mail from your home mailbox every day. If you leave town, have the post office hold your mail or ask a neighbor to remove it daily for you.

Charity Solicitations

Description of the Scam

Crooks pretend to represent or mimic real charities and collect money for themselves. These scams tend to be particularly active during the end of year holiday season and following a natural or human disaster. The charity may or may not sound familiar. They may reach out via phone calls, emails, texts, in-person charity collectors, social media ads or via websites that appear in searches.

Spot the Scam

The representative may pressure you to contribute immediately.

You may be asked to make a check payable to an individual, rather than an organization.

The organization is not listed at <https://apps.irs.gov/app/eos/> as an IRS 501(c)(3) tax deductible agency.

Note that crowd-funding (such as gofundme) donations are not IRS-recognized charities and therefore donations to them are not tax deductible.

Stop the Scam

Only donate to charities you've heard of or have researched, even after a disaster or tragedy. Make sure you're using a verified website or phone number that you locate on a legitimate website or other source, not one provided in a call or message you receive.

Don't open emails or texts that you suspect are hoaxes. If you open one that looks suspicious, do not click links and immediately delete it. You can also report it as spam or junk and block the sender from contacting you again.

Do not let callers or emails press you into giving money at once.

Clarify to whom the check or credit card will go. Never make a charity check or payment in a specific individual's name.

Investigate charity crowd-funding campaigns and other organizations before donating. Request details in print about the organization, including its mission and financial statements, location, where donated money goes, and written verification that donations are tax-deductible.

Do not provide credit card, social security or bank account numbers to someone who contacts you for a donation. If, after researching the cause, you decide to donate, use contact information on the verified website that you locate independently.

Do not pay in gift cards or cash.

Prevention

Before donating, research charities through the Massachusetts Attorney General's Office Division of Non-Profit Organizations and Public Charities as well as the Better Business Bureau's Wise Giving Alliance. Give through using the organization's official website.

Only donate to respected, well-known organizations.

Credit, Debit and SNAP Cards

Description of the Scams

Card skimmers may be inserted into machines where people pay in person with credit, debit, and SNAP cards. These devices capture card information, including numbers, signatures, and PINs. Thieves use this information to steal money.

Other credit card scams include:

- Charges by someone not authorized to use your card.
- A false notification that a lower interest rate is available if the individual pays a lump sum immediately.
- Someone nearby steals credit card information electronically while it is in your wallet or purse.
- The card holder is falsely notified that they were overcharged for an item and will get a credit once they provide/confirm the number.

Spot the Scams

If the keypad buttons of a machine are stiff when you start to enter a PIN or amount, it may indicate that an object has been placed over the original keypad.

If the slot where you insert your card is not flush to the machine, there may be an insert.

Stop the Scams

Before sliding your card into the apparatus to pay, check if the around the device's insert slot is loose. This is true for all machines, particularly those that are not always attended, such as ATMs and gas pumps. Inform the Brookline Police at **617-730-2222** if you notice anything suspicious. (Notifying employees may not be effective, as they may have installed the skimmers themselves.)

If you get a call or message notifying you to contact the firm that issued your card, call the number that is on the actual card (not a number provided in the message).

Do not provide your PIN or account password to anyone. If someone requests it, call the number on your card and notify the issuer that this occurred. Change SNAP passcodes regularly.

If you spot a wrong charge on an account, notify the issuing business immediately.

Do not provide your credit card number to someone claiming to owe you a refund. Review your card statement to confirm whether amounts charged are correct. If you spot an error, contact the business directly using the contact information available on a verified website or other source.

Prevention

When using online accounts, choose passwords that are difficult for others to figure out. Do not utilize computer programs that automatically save and fill in passwords. If possible, enable 2-step verifications (such as having a code texted to your phone number whenever you log in) or fingerprint recognition.

Keep credit card numbers confidential, and only provide them when you contact a company or bank, not when they claim to be contacting you.

Photocopy or write down information from the front and back of cards you do carry around. File the copies in a secure location in case the originals go missing.

Do not carry around any cards (such as Medicare and Social Security) that you don't regularly need when you leave home.

Consider placing a limit on daily charges and withdrawals on all of your accounts.

Sign up to receive all of your statements electronically, or shred financial documents when you no longer need them.

Check your accounts regularly - as often as once a day, if possible - to ensure that there are no fraudulent charges posted.

Set up email or text alerts with your banks and credit card customer service departments to be instantly notified of charges made on your accounts. They can notify you for all purchases or ones over a designated amount.

Notify the issuing institution immediately if you lose or misplace a credit/debit card.

Contact your credit/debit card company to opt-out of sharing your data. You can also ask for a copy of the information they keep on your card activity and request that they delete information on your spending.

Keep credit and debit cards, especially those that use tap technology, in secure RFID cases.

Data Breaches/Identity Theft

Description of the Threat

Hackers break into corporate databases and steal data such as names, addresses, birthdates, social security, and financial account numbers. They then may apply for credit, place charges, withdraw funds, and/or impersonate the people whose information they have acquired, stealing from those people.

After a Breach

Here are some steps to take if you've been notified that your information may have been accessed by hackers:

- Verify that the report is legitimate through the Office of the Attorney General's website at <https://www.mass.gov/archive/data-breach-notification-letters>
- Change passwords and PINs associated with account information that may have been revealed.
- Set up a fraud alert through Equifax (Equifax.com), Experian (Experian.com), or Transunion (Transunion.com), indicating that future accounts created in your name go through an extra verification process in order to be activated. (By notifying any one of these credit bureaus, an alert will be placed on all three.)
- Enroll in credit monitoring, often available free of charge, through Equifax, Experian, and Transunion.
- Access a free credit report through annualcreditreport.com. You can get one a year from Transunion and Experian; Equifax may offer more than one report annually.
- Consider freezing or locking access to your credit history, as well as your dependents', through Equifax, Experian, and Transunion.
- Watch for signs and notifications of charges, accounts, and actions that you did not generate. If you notice suspicious or unexpected activity, **contact the Police at 9-1-1 and the National Elder Fraud Hotline at 833-372-8311**. Also notify financial organizations (such as banks, investment and credit card agencies), that you have experienced identity theft and request that a fraud alert be placed on all of your accounts.

Spot a Hack

If you receive an unexpected authorization code via text, ignore and delete the message. If you receive one by email, immediately change your email password.

Prevention

There is no fool-proof way to ensure that your information will be safe from hackers. However, the following steps can minimize risk.

Change all passwords at least twice a year. Choose substantially different passwords for each account. Do not use ones that are easy to guess. Instead use random words. (You can write them on a list kept in a secure place or use a secure online password keeper app.)

Use multifactor authentication (which, in addition to requesting your password, requires a code sent to your phone) to log into online accounts.

Choose different passwords for each account.

Do not save credit card numbers on websites for future online transactions.

Install, update, and regularly run antivirus programs on your devices.

Minimize providing your phone number to open accounts. If possible, delete it from the record once the account has been established.

You can preemptively freeze or lock your credit through the credit reporting agencies (Equifax.com, Experian.com, Transunion.com) to minimize future fraud. This is especially recommended for children's credit (as their accounts are not monitored as frequently). The freezes can be temporarily lifted and re-installed when consumers apply for loans. Note that freezes are by individual, so when there are joint accounts, each individual's credit needs to be frozen separately.

When browsing online, do not accept tracking cookies. If that option is not available, accept only necessary cookies.

To find out if your data may have been compromised, you can access a list of companies experiencing data breaches at: <https://www.mass.gov/lists/data-breach-notification-reports>

Decline offers to utilize consumer loyalty apps in exchange for rewards. These often collect and sell user information to other companies.

Maximize privacy on your cell phone by turning off features such as location detection (except for times you need it for driving directions) and app tracking. iPhone users can find a list of steps to take at <https://pirg.org/edfund/resources/iphone-privacy-settings/>

Change the default password and SSID (service set identifier) that came with your home internet modem router. For both, use words that would be difficult for someone to guess and associate with you (not your name).

Investments, Bitcoin and Other Cryptocurrencies, Loan Approvals

Description of the Scams

The person receives a call, message, or sees a social media post about a great investment, sometimes deceptively appearing to be in or by a well-known company. Or the offer may promote investment in bitcoin or other cryptocurrencies. When people fall for this pitch, it may initially appear that they are getting amazing returns on their money.

Alternatively, the recipient may be told that their bank account has been accessed by thieves and that it's crucial to withdraw all of their money in cash and convert it to cryptocurrency. The money actually gets deposited into someone else's account.

People posing as stock brokers, real estate developers, or precious metals dealers may promise very high returns, and may indicate that profits are guaranteed.

However, these may be misleading fake "Ponzi Schemes."

In related ploys, the individual may be informed that they've been approved for a loan. Sometimes they are asked to pay a processing fee.

The investment/loan is a sham, and the individual loses their money.

Spot the Scam

Scammers may press the potential investor to act quickly or they will lose out on this opportunity. They could threaten that the stock market is about to crash and that the government will shortly take over everyone's retirement funds or that their bank savings are at risk.

Be suspicious if the stated investment return rate seems too good to be true. Or if the value rises sharply, which may be followed by an abrupt crash.

The person may be instructed to withdraw cash (often significant amounts) from their bank immediately and deposit it into a specified ATM, sometimes referred to as a "Crypto Kiosk". (It may not be apparent that the particular machine converts cash to cryptocurrency.) These machines may be located in unlikely places, such as gas stations, convenience stores, or supermarkets. The person offering the "investment" may encourage their prey to stay on the phone with them while they are making the transaction to ensure it is processed.

Stop the Scam

Legitimate investment brokers, dealers, and investment advisors must be registered with the Massachusetts Securities Division. Contact the Division at 1-800-269-5428 or 617-727-3548 to check credentials and verify the individual or company before providing funds.

Don't fall for time pressure.

Never invest in cryptocurrency upon the invitation of a company you haven't previously heard of or an individual you've never met in person and/or do not know well (including if you are having an online romance with them).

Don't invest more money than you can afford to risk losing.

Get as much information about the investment as possible before committing. Be careful if it's difficult to get details.

Do not invest using an ATM or Crypto Kiosk.

If You May Have Been Scammed

Notify the Brookline Police at **617-730-2222**.

Contact the Massachusetts Attorney General's Office at **(617) 727-8400** or online at <https://www.mass.gov/how-to/file-a-consumer-complaint>

You can file a complaint with the Massachusetts Securities Division at <https://www.sec.state.ma.us/InvestorComplaint/compidx.aspx>

Prevention

Investigate loans, grants, investments, or other financial assistance that you are offered or hear about. Look for government programs that do not charge.

P2P Phone/Electronic Payments

Description of the Scams

Scammers pose as sellers or a company stating that you owe money and demand payment using an app such as Zelle, Paypal, and Venmo. These transactions are nearly impossible to cancel or reverse once completed.

Spot the Scam

The request for money may have urgency, such as an immediate payment deadline.

Stop the Scam

Do not respond to pressure from phone calls or messages. Research the company or seller before making payment. Confirm that you owe the amount stated using a verified phone number or genuine website.

Prevention

Send money only to sources you know and trust. Ascertain directly with the recipient that you have their current valid contact information. Ensure that you spell their email and account information correctly. You can make a small trial payment of \$1 and then confirm receipt directly with them before sending the full amount.

Have a unique, nonsense password for each account. Set up multi-factor sign-ins.

Set your account to private or friends only to keep your transaction history from being easily accessible to the general public.

Do not give anyone account or password information.

Create an alert to be notified of activity in your account. Scrutinize financial statements often.

Government Scams

EZDrive Electronic Toll Payment

Description of the Scam

People receive text or email messages that appear to originate from the Massachusetts Department of Transportation (MassDOT) EZDriveMA (or a similar agency) demanding payment for highway tolls with a link for payment. This is a false message, and the link brings people to a bogus website.

Spot the Scam

EZDriveMA does send text messages requesting money.

If the link provided does not begin with **www.EZDriveMA.com**, it is a hoax.

Stop the Scam

Notify the IC3 at **www.ic3.gov** about this message. Provide the phone number or email of the message sender, as well as any websites included in the message.

Contact **www.EZDriveMA.com** or **877- 627-7745** to verify whether you owe money.

After filing a report, delete the message received.

If you clicked on the link and provided information, alert your financial institution that you may have been the victim of a scam so they can help you take any necessary precautions (such as stopping payment or changing account numbers).

IRS/Tax Returns

Description of the Scam

People impersonating IRS workers state that the individual owes tax money and will be arrested or deported unless paid immediately. The person reaching out may offer to consolidate debts for a fee. These are scammers trying to get money.

Another racket occurs when swindlers file false tax returns using someone's birth date and social security number. They may have the refund or stimulus money sent to them. Alternatively, they send money to your account and contact you pretending to be the IRS workers insisting you to return overpayments.

Spot the Scam

The IRS will not call to request personal information.

Be suspicious if this is the first time you have been notified about owing tax money with threat of imprisonment. The IRS makes a number of attempts to acquire payment before threatening consequences, and will not imprison or deport people.

The message is false if the request is for payment in gift or iTunes cards.

The IRS will not demand an extra processing charge.

Be alert for the following notifications from the real IRS stating that:

- They have received your tax return before you submit it.
- They have received two or more returns under the same social security number.
- They state that you did not report your complete earnings, citing income from an employer where you did not work.
- Confirmation of an online account that you did not establish.
- Confirmation of an Employee Identification Number (EIN) that you didn't request.

Stop the Scam

If you get a call that appears to come from the IRS, hang up.

Do not provide bank account, credit card numbers or other information to strangers.

Do not pay taxes in gift cards.

Prevention

File income tax returns as early as possible. Filing electronically may be safest.

Check the status of tax returns at <https://www.irs.gov/refunds/>

Ask your tax preparer how they safeguard your data and make sure you are comfortable with their precautions.

Request an IRS Identity Protection PIN at <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

Secure your personal and financial paperwork, and shred what you do not need.

Use up-to-date security programs on your computer.

Make sure your passwords differ for each online account and frequently change them.

Do not carry your social security card or number with you.

Do not use shared or public Wi-Fi for personal or financial transactions and communications.

Only provide sensitive information on websites that contain addresses with <https://> or display a padlock icon 

If You Suspect Fraud

Submit an IRS Identity Theft Affidavit (Form 14039, available online) at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>

Jury Duty

Description of the Scam

A call comes in, often with caller ID that indicates that it originates from a courthouse or police. The caller threatens to immediately arrest the individual for not showing up to jury duty as mandated unless a fine is paid. This is a sham call after money and/or personal data that will enable thieves to steal an identity and/or cash.

Spot the Scam

The person is told that they owe a fine, often requested via wired payment, gift or prepaid cards. The caller may ask for birthdates, social security numbers, or other information to “verify” the individual’s identity.

Genuine notifications for missed jury duty are always initially sent by mail. Court staff will not request birthdates, social security or license numbers.

Stop the Scam

Hang up immediately on anyone stating that they are from a courthouse or police. Do not provide personal information.

Do not be fooled by caller ID displays, these can be false.

Call the courthouse directly via a number listed on a legitimate website (not the number displayed on Caller ID or that the caller offers) to substantiate the claim that you missed jury duty.

Report the call to Norfolk District Attorney’s Office at **781-830-4920**.

Medicare

Description of the Scams

Scammers attempt to get access to individuals' Medicare numbers so they can place phony charges in the cardholder's name. These may include health care devices, such as catheters and knee braces.

Bogus agencies may inform people that for a fee they will stop medical debts from affecting one's credit rating. Or they may state that they can ensure individuals won't have to pay certain medical expenses. They may apply pressure tactics such as a looming deadline to enroll in this service.

Another scheme is selling an insurance or drug plan without disclosing that it has not been approved by Medicare.

Medicare may be charged for services or equipment you did not order or receive. Or the culprits may bill twice for something you attained one time.

Spot the scams

Scams include calls or messages that falsely appear to originate from Medicare.

Examples are:

- A caller states that they need a Medicare, Social Security and/or credit card number to send information on plan options and/or enroll you in a plan.
- You are falsely notified that you need to enroll in a Part D Prescription Drug plan to be eligible for Medicare.
- You are told that Medicare has to verify your billing information so you can stay insured.
- A person introducing themselves as an insurance agent offers supplemental insurance/ Medigap or a Medicare Advantage plan at an amazing price.
- Someone claims to be from Medicare and asks you to pay for your Medicare Card.
- A "salesperson" convinces you that you need a brace or other medical equipment or services (such as house cleaning or home nursing care) that was not prescribed. They request your Medicare number. They employ dishonest doctors, and charge Medicare for a device that isn't needed.
- A health fair "representative" offers genetic testing for cancer or other hereditary diseases. In order to participate, they request Medicare numbers, then illegitimately bill that account. (They often do not provide test results information as promised.)
- Your Medicare statement reflects charges for items you did not order.

Stop the Scams

If someone calls claiming to be from Medicare and/or requesting your account number, hang up immediately.

Never provide the Medicare number to someone who has called you.

Medicare will never call people to enroll them. They also will not request payment over the phone or email.

Be assured that Part D plans are optional, and people can be enrolled in Medicare without participating in a Part D insurance.

There is no charge to receive a Medicare card and number.

If someone contacts you claiming to be an insurance agent, do not provide card numbers, personal information or "enroll" over the phone. If the offer sounds interesting, request that the company send you written information. Contact the State Attorney General's Office at **617-727-8400** to confirm that the insurer and agent are authentic. Feel free to ask someone you trust to review information you receive to see if it appears to be legitimate.

Do not click on an email link unless you're sure of its source.

Thoroughly review your Medicare Summary Notices and charges to confirm that they align with the services and/or supplies you received. Make sure that the correct dates are listed. Notify Medicare of charges for treatments or goods you did not receive by calling **1-800-MEDICARE (1-800-633-4227)**. You can report suspected fraud to the Department of Health and Human Services through <https://oig.hhs.gov/fraud/report-fraud/>

Prevention

Keep your Medicare card and number in a safe place.

Permit only your personal care providers, such as doctors and therapists, to access your medical history and suggest treatments.

Discuss Medicare enrollment options exclusively with trusted, unbiased sources such as through **Medicare.gov**, the Medicare hotline at **800-MEDICARE (800-633-4227)** or a verified SHINE counselor at the Brookline Council on Aging (appointments can be made at **617- 730- 2777**).

Natural Disaster Survivors

Description of the Scam

Dishonest people may try to benefit from victims of disasters. One ruse is posing as workers who will clean up destroyed property. Another is charging fees to submit applications for FEMA funds.

Some scammers impersonate owners of rental properties for survivors in need of temporary emergency lodgings.

Spot the Scam

Scammers may quote excessively high rates and/or expect to be paid before any work is done.

Culprits may offer to help survivors apply for FEMA funds at a cost. FEMA does not require fees to apply for money.

People offering temporary housing may demand money before the individual has seen the residence.

Stop the Scam

Do not provide personal information to callers or people showing up at your door, even if they claim to be with the Federal Emergency Management Agency (FEMA).

Do not believe someone saying that FEMA sent them to make repairs. FEMA does not use or recommend specific contractors or companies. They also do not provide vouchers.

Do not believe someone who states that they can negotiate with FEMA to provide additional assistance.

If someone claims to be a public insurance adjuster who can assist you, do not pay them upfront or provide any personal numbers, such as social security or bank accounts. For more information on safely working with an adjuster, look at; <https://www.mass.gov/doc/consumer-alert-public-insurance-adjusters-062011/download>

Do not pay in cash, gift cards, cryptocurrency, or wire transfer.

Never provide your social security or bank account number.

Prevention

Only contact agencies on official government websites.

Always request workers' identification, insurance information and licenses. You can call the Massachusetts Attorney General's Office (AGO) Consumer Hotline at **617-727-8400** to get information about specific companies and workers.

Get work agreements in writing.

Pay the final installment for repairs only after all of the agreed upon work is completed to your satisfaction.

Police and Homeland Security Scams

Description of the Scam

Residents receive calls that appear to come from the Police or Department of Homeland Security stating that they have data on the individual. They may leave a message requesting that you call back a specific number.

Spot the Scam

Callers may threaten to arrest the individual unless the person pays them.

Stop the Scam

If you answer such a call, hang up. If you receive a message indicating that you need to call the police at a specific number, do not call that number.

Report these calls to the Brookline Police at **617-730-2222**.

Prevention

Be wary of unexpected calls from the Police, even if your caller ID says that's the origin and the phone number appears to be correct.

Verify the identification of anyone showing up in person claiming to be law enforcement. Call the Police at **617-730-2222** to confirm that they are legitimate.

Postage Stamp Scams

Description of the Scam

Ads on websites such as Facebook and eBay claim to sell postage stamps at a discounted price. The stamps are fake. Mail posted with such stamps may be confiscated and reported to the US Postal Service.

Spot the Scam

An online ad will offer a bulk order of stamps at a discount (such as \$39 for \$58 worth of postage).

Stop the Scam

Don't fall for these ads.

Prevention

Always buy postage stamps directly through the post office or an authorized sales location.

Social Security Scams

Description of the Scam

Scammers impersonate Social Security Administration staff in order to gain access to people's funds and/or Social Security numbers (to establish false accounts).

Spot the Scams

A call, letter, text or social media message that appears to come from the SSA dishonestly states that a crime (such as selling drugs or sending money overseas) was committed using your Social Security number. The notification may appear to be on official government letterhead. It might claim that the account has been blocked, and that you need to pay a fee to get it reopened. Or they may ask to verify your Social Security number.

A message that seems to be from the Social Security Administration falsely indicates that your Social Security number has been stolen and used by thieves to apply for credit cards, and that you are at risk for losing your benefits. It could state that your bank account will be seized unless you follow their instructions for keeping it safe.

Someone claiming to be from Social Security says that the recipient has to pay back money or has additional funds coming their way. They then ask for the Social Security number to process the information.

Stop the Scam

The SSA will not ask for your Social Security number, money, or to tell you that your benefits are at risk.

If it's a call, hang up. Do not respond to these emails or texts. Do not give out your Social Security number (not even the last 4 digits), bank account, or credit card number to people who contact you for it.

Do not wire money, send cash or pay with gift cards to anyone who reaches out to you – including those claiming to be from the government.

Notify the real SSA about the call at **1-800-772-1213**.

You can also register a complaint with the Federal Trade Commission at **[ftc.gov/complaint](https://www.ftc.gov/complaint)**

Unemployment

Description of the Scam

Impersonators who have stolen identity information place false unemployment insurance claims, directing the money to themselves.

Spot the Scam

You may receive notification from the Department of Unemployment Assistance that you have opened a claim when you did not.

Or you may get a 1099-G form reporting unemployment insurance income that you did not attain.

Stop the Scam

Report the fraud by completing a form at **<https://www.mass.gov/info-details/report-unemployment-benefits-fraud>**

Notify the Police at 9-1-1.

Veteran and Military Scams

Description of the Scams

Messages and postings on social media target veterans, claiming to offer assistance in attaining benefits due as a result of exposure to toxins during their service. These are a ploy to get information and/or money.

Thieves often target people currently serving in the armed forces. Their bank or credit card information is stolen more frequently than the general population.

Stop the Scam

Always investigate the qualifications of people offering assistance in filing an application with the Veterans Administration. You can use the Department of Veterans Affairs Accreditation Search tool at <https://www.va.gov/ogc/apps/accreditation/index.asp>.

Check your financial accounts regularly to ensure there are no suspicious transactions. Promptly contact your bank regarding any unauthorized activity.

Report suspected identity theft to the FTC at <https://www.identitytheft.gov/>

Prevention

Enroll in no-cost identity and credit tracking for service members through Equifax, Experian and Transunion. You can also request a free active-duty fraud alert with any one of these companies. They, in turn, will notify the others.

You can temporarily suspend credit and debit cards not in use while on active duty through your bank mobile app.

Know that there is no charge to file benefits claims due to exposure to toxic substances.

You can get information on free assistance in filing a claim at: <https://benefits.va.gov/vso/index.asp> Applications may be filed directly at: <https://www.benefits.va.gov/BENEFITS/Applying.asp>

Veterans can learn more about the PACT Act at: <https://www.va.gov/resources/the-pact-act-and-your-va-benefits/>

HOME

Home Refinancing

Description of the Scam

Offers through email, phone calls, and flyers claim to help homeowners refinance to low-interest mortgages for a fee. Scammers steal any money they are given, as these claims are false.

Spot the Scam

The notifications indicate that these low-interest loans are available for a short time (with terms such as “limited time offer” or “act fast”) to pressure people to fall for the scam.

The notice may appear to be connected to an initiative by the government or another well-known agency.

They may demand that recipients terminate mortgage payments to their present lender.

Sometimes these notices are aimed at people who are behind on paying their mortgages and particularly vulnerable.

The interest rate offered may seem incredibly low.

Stop the Scam

Be wary of unexpected contacts from an organization that sounds unfamiliar.

Be particularly suspicious if the offer appears to be an unbelievably good deal.

Do not provide callers with any information such as account numbers.

Before making changes, inform your current mortgage lender via a verified phone number about the offer. They can also help people who are late or behind in their payments.

Refrain from taking impulsive actions. Consider a number of trusted alternatives before refinancing.

Notify the Massachusetts Attorney General’s Office Consumer Hotline at **617-727-8400** or the Elder Hotline at **888-243-5337** about the communication you received so they can verify and/or probe the offer.

Home Repair, Improvement, Contractors

Description of the Scam

Someone states that they are in construction and can fix something around the building they notice is in disrepair (such as masonry, a driveway, roof, chimney, landscaping).

They may come by in person, call, place ads, or distribute flyers. Or they may be found online via false websites with fake information and reviews.

Sometimes they complete smaller tasks before offering or agreeing to take on major projects. In the end, they take the person’s money and do not complete the work as promised.

Another scheme is to pose as workers and steal people’s possessions.

Spot the Scam

The offer may claim to make repairs at amazingly low prices.

Often there is pressure to immediately commit to having the work done to get the best price or before the situation gets worse.

Scammers can claim the price is so low because they have materials leftover from another project.

The “workers” may ask for full payment before starting the project. Or they may insist on getting paid in cash, gift cards, or other unconventional means.

The name of the business may not be included in the ad or phone call.

Listed references may be from a faraway location; online reviews may all have been posted around the same time.

The offer is unclear or confusing.

If a building permit is necessary, the worker may falsely state that it is the homeowner’s responsibility to file the paperwork.

Stop the Scam

The Brookline Police need to provide prior approval to anyone selling items or services door-to-door. Contact the police at **617-730-2222** to confirm that they have approved this person’s activities.

Always research companies on sites such as the Better Business Bureau prior to engaging them.

Confirm that a business is licensed through the Massachusetts Office of Consumer Affairs and Business Regulation at <https://services.oca.state.ma.us/hic/licenseelist.aspx>

Contact more than one company to get estimates for the job.

Ask workers to provide documentation of current insurance.

Make sure you have a signed contract before paying anyone to do work. Ask someone you trust to review and explain contracts before signing. Do not sign anything that is unclear or difficult for you to comprehend.

Do not pay in full for repairs until a project is complete.

Never pay in cash.

Invite someone you know into your home while the work is being done to ensure safety of yourself and your belongings.

If you have been swindled, notify the Brookline Police at **617-730-2222**.

Prevention

If you need to make repairs, ask people you know for worker recommendations.

Home Warranty

Description of the Scam

A letter appearing to be a bill, possibly pertaining to the person's mortgage, states that a home warranty is expiring or has expired. It indicates that action is urgently needed, and provides a number to call and verify information. This is actually a marketing ploy to sell services.

People may receive this information via phone calls or online messages as well.

Spot the Scam

The notice indicates that your warranty is expiring, even though you may not have previously purchased a warranty for your home. Or you already have one that is still current.

The letter may state "Immediate Response Requested" and/or that this is a "Final Warning."

There may be a voucher attached that looks like a check.

Stop the Scam

Do not call the phone number.

Prevention

When purchasing a home or property, opt-out of having your information shared for marketing purposes.

Home warranties for appliance repair are optional. If you would like one, research legitimate companies via the Better Business Bureau and other trusted sources before buying.

Homeowner Deeds

Description of the Scam

A letter arrives stating that people can attain an official copy of their real estate deed for a charge. Sometimes this appears similar to a bill with a due date.

Spot the Scam

Copies of Brookline property deeds are available for free at www.norfolkdeeds.org.

Certified copies can be requested at this site for about \$3.00

Stop the Scam

Do not respond to the mailing.

Verify information with the Norfolk County Registry of Deeds at **781-461-6101** or registerodonnell@norfolkdeeds.org

Trash with Personal Information

Description of the Scam

Crooks go through trash looking for information such as credit cards, account numbers on receipts or bank, and account (pre-) approval notices that they can use for their own benefit.

Prevention

Shred documents and envelopes that contain identifying information - from your name and address to account numbers and dates of birth. The Senior Center has an annual shredding day where you can bring your documents in person. In addition, some people cross out information on both sides of documents using wide felt tip pens (such as a “Sharpie”) and/or special stamps.

Cut up old credit and debit cards before tossing them.

Utility Callers and Workers

Description of the Scam

An imposter claims to be the utility company threatening to turn off power unless paid immediately. (The phone Caller ID may misleadingly list the actual company name.)

Or someone claiming to be a utility worker may show up at your home when you are not expecting them. They may claim to need access to do work or that they are offering opportunity to get service from a different energy company.

Spot the Scam

Fraudulent callers may not have your full account information.

They often insist on being paid through credit, debit, or gift cards.

The caller sounds angry or insistent.

Customers cannot be threatened with services being turned off in their first notification that an account is past-due. (They must be contacted several times before this consequence can occur.)

Stop the Scam

Request official identification from anyone appearing in person claiming to be a utility worker, particularly if their visit was unexpected. Call the utility company before admitting them to verify that the person is legitimate.

Do not give payment to someone appearing in person.

Do not pay a caller with a wire transfer, prepaid gift or credit cards. Hang up if the caller becomes demanding.

Call the utility company using a legitimate phone number on the verified website or recent bill to verify the situation.

Notify the Department of Public Utilities at **617-305-3500**.

Contact the Brookline Police at **617-730-2222**.

TECHNOLOGY

Computer Virus, Malware Notification

Description of the Scam

Messages are sent falsely stating that electronics are infected. The computer may in fact be fine, but clicking on links or calling the numbers listed may then install computer malware. Or scammers may take control of your device from another location. Alternatively, they may charge to needlessly “repair” the computer.

Spot the Scam

A window pops up onscreen stating that the computer or phone is infected. An alarm or siren may sound. A phone number or link to click are provided.

A sign of infection is the sudden inability to utilize apps or programs and someone demands that you pay them to resume access to them.

Other indications are a sudden slower processing speed, more pop-ups, and unrelated websites appearing during online searches. Also, antivirus programs may no longer function.

Stop the Scam

Do not call the number or click on the link listed. Follow the directions below.

Do not provide permission to take over your electronic device remotely, even to people who seem to offer assistance.

If You Suspect Your Machine Has Been Infected

Do not pay anyone to ransom your device.

Do not turn off your device, disconnect it from the internet, open or close windows.

Using another device (the Senior Center staff can assist you), notify the Internet Crime Complaint Center at <https://www.ic3.gov/> or the local FBI office at [boston.fbi.gov](https://www.boston.fbi.gov/), **857- 386-2000**.

Contact a reputable computer support service that you locate on your own or with assistance from someone you know to confirm whether there is a problem with your technology and, if so, how to remedy it. You can call the Brookline Senior Center at **617-730-2777** to schedule a meeting with a Technology Consultant.

You can try unplugging from the internet, shutting down Wi-Fi, and using your device offline in Safe Mode. You may then scan the machine with previously installed antivirus and anti-malware programs. When you go back online, immediately change all passwords.

Prevention

Install and consistently update antivirus and anti-malware programs on your devices.

Change your online passwords regularly.

When using a password or creating a new one, do not agree to have the computer save it when prompted. Instead, use a password manager (such as Google, Nordpass, and KeePass).

Do not respond to surveys (customer service, transportation, social media “personality tests”).

Do not use the Telegram app, as it can allow others to take over your cell phone.

QR (Quick Response) Codes

Description of the Scam

Deceptive QR codes that look legitimate can infect devices or lead users to sham websites that access identity information.

Spot the Scam

An email or message that appears to come from a familiar, established company indicates that the recipient should promptly scan the included QR code.

A QR code has been pasted over older (real) ones in locations such as parking meters and posters around commercial areas.

Stop the Scam

Do not scan QR codes provided in unexpected messages. Reach out to the company directly using contact information provided at their legitimate website if you're concerned that the notification may be true.

Carefully check the URL provided to ensure that it is the correct one for the business before opening the link. If it doesn't look familiar, don't use it.

Prevention

Confirm that your devices are using the newest operating systems. Make sure you have strong passwords and multi-factor sign-ins for your accounts.

Wi-Fi Public Internet Access

Description of the Scam

Individuals trying to access the internet in public spaces may be charged by scammers posing as businesses asking for a fee.

Prevention

Before accessing a public internet network, attain information from an employee at the location to confirm the official network and any associated cost.

Do not use financial or personal websites on a public or shared network.

If possible, use a VPN service for security.

Information Sources For This Publication

AARP Fraud Resource Center <https://www.aarp.org/membership/benefits/finance/fraud-resource-center/>

Better Business Bureau

Boston Globe

Brookline Bank

Brookline Police

Commonwealth of Massachusetts (2023) *A Consumer Guide to Scams*
<https://www.mass.gov/guides/a-consumer-guide-to-scams>

Consumer Affairs

Experian

Federal Communications Commission

Federal Trade Commission **ftc.gov**

IDX

JVS of Metrowest

Massachusetts Securities Division

The Massachusetts State Attorney General's Office

Medicare

National Council on Aging

Norfolk County District Attorney's Office

Norfolk County Registry of Deeds

Pension Action Center

Rockland Trust

Social Security Administration Office of the Inspector General

Teachers Insurance and Annuity Association of America-College Retirement Equities Fund

Upgraded Points

United States Department of Health and Human Services

United States Federal Bureau of Investigations

United States PIRG

United States Postal Service

Index–Common Types of scams

Banking.....	22	Letters from Santa	8
Bereavement and Obituaries	18	Lotteries, Contests, Sweepstakes Winners	9
Bill Paying by Check.....	23	Medicare Scams.....	31
Celebrity Messages.....	8	Natural disaster survivors targeted.....	32
Charities.....	23	Obituary notices – keeping personal information safe	18
Clergy Messages	19	Online Dating/Romance.....	9
Computer Virus, Malware Notification	40	Online shopping.....	14
Credit, Debit and SNAP Cards	24	P2P Phone/Electronic Payments	28
Data breaches/identity theft	26	Package delivery.....	15
Emails	7	Phone calls; robocalls, one-ring hangups.....	5
Facebook and Social Media	19	“Police” scams	33
Family/Friend Emergency.....	21	Postage stamp scam.....	33
Genetic Screening/Testing.....	13	Purchasing Gift Cards.....	14
E-Cards (Online Birthday and Greeting Cards).....	13	QR (Quick Response) Codes.....	41
EZDrive Electronic Toll Payment.....	29	Social Security	34
Florists.....	13	Streaming TV and Movie Entertainment	17
Home Refinancing	36	Text Messages (“Smishing”).....	7
Home Repair, Improvement, Contractors.....	36	Tickets for Shows and Sport Events.....	17
Home Warranty.....	38	Trash with Personal Information	39
Homeowner Deeds.....	38	Travel and Vacations.....	10
Investments, Bitcoin and Other Cryptocurrencies, Loan Approvals	27	Unemployment Benefits	34
IRS/Tax Return.....	29	Utility Scams.....	39
Jury Duty Scams.....	30	Veteran and Military Scams	35
		Wi-Fi Public Internet Access	41

Information for this publication was compiled and edited by Miriam Rosalyn Diamond

Published by:
The Brookline Council on Aging/Senior Center
 93 Winchester Street, Brookline, MA 02446
(617) 730 - 2777

BROOKLINE SENIOR CENTER SPONSORS OF THE 2023



Autumn Benefit

Thank you for supporting the BROOKLINE SENIOR CENTER

The Senior Center could not do what it does without you! More than you can ever imagine and more than we can ever express, the Brookline Senior Center is grateful that you are a part of this vital work.

This publication was made possible due to the generosity of our sponsors.

Diamond

Beth Israel Deaconess
Medical Center
Elaine K. Kwiecien
Doris Toby Axelrod and
Lawrence Marks
Michael W. Merrill
Suburban Home Health Care

Ruby

Anonymous
Brookline Rotary Club
Carol Caro
Goddard House Assisted Living
Shulamit Kahn and Kevin Lang
Betsy Pollock
Hanson Reynolds and
Sharon Gray
Richard and Winnie Rubino
Sherrill House
Suzanne Salamon and
Alan Einhorn
Waterstone At The Circle

Sapphire

Ruthann Dobek and
Glenn Boghosian
Patricia H. Dobek

Emerald

Anonymous
Atkin Associates, LLC
Christina Cunningham
Mady and Bruce Donoff
Victoria Fremont
Barr and Joyce Jozwicki
Levine Chapels
Mojtaba Mostashari
Ruth K. Seidman
Neil and Susan Wishinsky
Sonia and William Wong

Topaz

Brookline Hearing Services
Brookline Municipal
Credit Union
Margolis Bloom & D'Agostino
Ellen A. Bruce and
Richard Segan
Helen Charlupski
Eleanor Clarkson
Carolyn and Ted Colton
Morgan and Rita Daly
Nancy Daly and
Kevin Cavanaugh
Doris K. and Saul J. Feldman
Pamela Hitchmoth
Home Instead
Bruce and Georgia Johnson
LaPointe and Days LLC
Alberta and Roger Lipson
Mount Pleasant Home
The Move Maven
Mary M. Mullarkey
Judy Meyers and
Mark Pasternack
Providence House
Carol and Morry Sapoznik
Barbara and David Westley

Opal

Pat Ahlin
Saralynn and Alan Allaire
Always Best Care
Fay Andreadis
Anonymous
Diane Baker and
Edward Baker III
Jerald and Devora Baronofsky
Ros Barron
Christina Wolfe and
John Bassett
Dorothy (Dotty) Bell

Brookline Booksmith
Dorothea A. Brown
Carole Chang
Janie Chickering
(Clara) Lai Bing Chin
Jewel Chin
Martha Curtis
Eugene and Eva
Balash Deutsch
Daniel H. Ferguson
Franklin and Maria Ferguson
Livia Frank
Marion Freedman-Gurspan
Leslie Friedman
Zelda Gamson
Laurence and Yurika Geffin
Barbara Goldwasser
Bambi and Michael Good
Hildy and Richard Grossman
Mary W. Haas
Gerry Hayes
Regina Healy and
Robert Sloane
Helen and Shael Herman
Faye Jordan
Margie and Ed Kahn
Marie Claire Kamin
Judith Kidd
Edward F. King
Joan Lancourt
Juliette Landesman
Chi Chung and Toy Soo Lau
Sherry C. Lee
David and Ilana Lescohier
Arlene and Edward Levitt
Enid Lieber
Judith E. Mason
Patricia L. Meaney
Lynn Modell
Margaret Morrill

Soo Moy
John and Betty Mulhane
Opal-continued
Alisha Nanda
Amy Ruth Nevis
Bebe Nixon
Paula H. Noe
Mary O'Connor
Katherine Paget
Jennifer Pieszak
Adele W. Pike
Virginia Po
Rosamond Rabinowitz
Anne S. Reed
Sharon Sandalow
Lucy and Philip Sandler
Elizabeth A. Sands
Bernice Schotten
Toni Schroder
Marie and Frank Scurti
Judith E. Sher
Rita Shon-Baker
Michael and Rena Silevitch
Barry Small
Lorraine Stevens
Rebecca Stone
Jean and Peter Stringham
Carla Tardi
Joseph Trunk
Kea van der Ziel
Karen Van Kennen
Kent and Nancy Van Zant
John VanScoyoc
Doreen Vittori
Matthew and Ellen Weiss
Deirdre Whelan
Robert and C. Leah Winter
Joyce Wishnick
Sandra Wong
Helen Yee

Thank You for supporting Brookline's older adults!

Brookline Senior Center
93 Winchester Street, Brookline MA 02446
brooklineseniorcenter.org



Are you looking for a unique gift? Well, you are in luck! We are offering another fun way to find that perfect gift or treat yourself while providing much-needed support to the Senior Center. The Brookline Senior Center has opened up shop on Etsy – a global online marketplace for vintage, handmade, custom and unique items—under the name

BROOKLINE BAZAAR

Brookline Bazaar showcases a diverse collection of antique and vintage treasures and collectibles from around the globe- including many one-of-a-kind pieces. New items are added weekly.

100% of Brookline Bazaar proceeds go to support Brookline Senior Center

www.brooklineseniorcenter.org

In fact, your support has allowed us to provide many of our virtual programs including, our monthly ArtMatters membership videos, and Emily Brenner’s Combo Dance Fitness Class!

Click the following link to take a look around the shop:

<https://www.etsy.com/shop/brooklinebazaar>

MOUNT PLEASANT HOME

WORRIED ABOUT A SENIOR LIVING ALONE?

Gorgeous, compassionate,
HAPPY home
for seniors
who need a little help

All-inclusive & affordable!

Near the Brookline Border

617.522.7600 301 South Huntington Ave, Jamaica Plain, MA

www.MountPleasantHome.org

Home Instead.

To us, it's personal

**Enhancing the Lives of
Aging Adults and Their Families**

- Personal Care
- Alzheimer's & Dementia Care
- Transitional Care & Medication Reminders
- Respite Care
- Mobility Assistance

- Companionship
- Meal Preparation
- Light Housekeeping
- Errands & Transportation
- Hospice Support

440 Totten Pond Rd. #300
Waltham, MA 02451

Office 781-341-0153
www.HomeInstead.com/398

Each Home Instead® franchise is independently owned and operated. © 2021 Home Instead, Inc.



**MERRILL &
MCGEARY**

ATTORNEYS AT LAW



MERRILL & MCGEARY

LAW FIRM ESTABLISHED IN 1979

REAL ESTATE LAW

CONTRACT LAW

CONDOMINIUM LAW

COMPLEX ROUTE LITIGATION

MUNICIPAL & ADMINISTRATIVE LAW

REAL ESTATE DEVELOPMENT

We are committed to providing good, solid, practical advice at reasonable rates in a timely and responsive manner. Our experience in and out of the courts puts clients in the best position for success.

- Specializing in the representation of condominium, cooperative and homeowner associations
- Committed to providing good, solid, practical advice at reasonable rates in a timely and responsive manner
- Our experience in and out of the courts puts clients in the best position for success

CONTACT US: (617) 523-1760 INFO@MERRILLMCGEARY.COM

*Thank you, Ruthann and Betsy,
and the other staff and
volunteers who make the
Brookline Senior Center
the warm, welcoming home away
from home that it is.*

Suzanne Salamon & Alan Einhorn




Brookline Hearing Services
Specializing in the elderly, hearing aids, hearing loss, and hearing loss prevention.



**WE'RE HERE TO
HELP WITH YOUR
HEARING NEEDS!**

Make your appointment today!
Call us at
617.232.1299

Brookline Hearing Services
1842 Beacon St., Suite #403
Brookline, MA 02445
info@brooklinehearing.com
brooklinehearing.com



Providence House
Assisted Living at Corey Park in Brighton
Affordable Assisted Living for Seniors of All Incomes
617-731-0505 www.providencehouseassistedliving.com

LAPOINTE & DAYS LLC



1309 Beacon Street, 2nd Floor
Brookline, MA 02446
www.lapointedays.com
**Please call for an appointment:
617-738-1919**

Helping People Find Solutions.

Your Attorneys for Wills, Probate,
Real Estate, Medicaid/Long Term Care,
Gift Planning, and Estate Tax Planning

**ENRICH.
ENGAGE.
TOGETHER.**



Goddard House offers residents enriching everyday experiences aimed at promoting independence, inspiring curiosity and encouraging connection with others.

Schedule a tour today!



**GODDARD
HOUSE**

ASSISTED LIVING & MEMORY SUPPORT

165 Chestnut St, Brookline MA
617.731.8500 | GoddardHouse.org



Trusts are the Swiss army knife of estate planning, being used to accomplish any equally wide variety of goals. But they're widely misunderstood. *The Baby Boomers Guide to Trusts* explains how trusts work.

Boston | Norwood | Wellesley
www.margolisbloom.com
781-705-6400

**Planning to move?
Downsizing? Decluttering?**

Contact us for a free consultation!



info@movemaven.com 617.905.8400



**PRESERVING *traditions*
STRENGTHENING *faith***

Dignity

LEVINE

CHAPELS

470 Harvard Street, Brookline, MA
02446

617-277-8300 LEVINEChapels.com



BROOKLINE MUNICIPAL CREDIT UNION

Experience the Credit Union Difference...
Since 1939

See Us For Your Financial Needs

**334 WASHINGTON ST., P.O. BOX 470776
BROOKLINE, MA 02447-0776**

Telephone: 617-232-9410 www.brooklinecu.com Fax: 617-232-1462

HANDICAPPED ACCESS

The Town of Brookline does not discriminate on the basis of disability in admission to, access to, or operation of, its programs services, or activities. If you need special accommodations, contact the Council on Aging at 617-730-2777.



Brookline Community Aging Network

BrooklineCAN

is an all-volunteer organization that focuses on Brookline as a great place to live. It provides information for older residents that helps them remain engaged in the life of the community, and advocates to make Brookline an even better place to live for seniors and everyone. It is separate from but works with the Brookline Senior Center, the town's Council on Aging, and Age-friendly Cities Committee.

All Are Welcome

93 Winchester Street Brookline, Ma 02446

617.730.2777

info@brooklineCan.org



*The Rotary Club of Brookline is proud to support
the Brookline Senior Center
for its significant services to the Brookline community
and for enhancing the quality of life of Brookline's elder residents.*



*The Rotary Club of Brookline, est. in 1938, is part of a global network
of 1.4 million neighbors, friends and leaders
who volunteer their skills and resources to take action to meet community needs*

In These 7 Areas Of Focus



www.brooklinerotary.org



Atkin Associates LLC

STRATEGY • MARKETING • FUNDRAISING

Providing Mission-Driven Organizations Insights and Solutions for over 25 years

Barrie Atkin, president

Barrie@AtkinAssociates.com or 781.788.6600

BarrieAtkin.com

Inquire about a Complimentary Consultation

Atkin Associates will help you BE BOLD, CREATIVE and SMART



Our Return to Home™ program will take you from the hospital back home

135 S. Huntington Avenue, Boston, MA 02130

Our Return to Home™ program is designed to prepare patients to return to their homes as quickly as possible following a hospitalization. Exceptional short-term rehabilitation is delivered by our experienced in-house clinical team.



Program Provides:

- Personalized Rehabilitation Services
- Beautiful sunlit, 3,000 sq. ft. Gym
- 24-hour Skilled Nursing Care
- Nutrition Counseling
- Award-winning Music Therapy
- Wound Management
- Patient & Family Education
- Family Care Plan and Discharge Planning Meeting



Sherrill House also provides long-term care, Alzheimer's and Dementia care, Longwood Hospice, and a Dialysis Den coming soon!

 [facebook.com/sherrillhouseinc](https://www.facebook.com/sherrillhouseinc)

 [@sherrillhousesnf](https://www.instagram.com/sherrillhousesnf)

(617) 731- 2400

www.sherrillhouse.org



PREMIER

SENIOR LIVING IN BOSTON

Ideally located at the foot of Chestnut Hill, Waterstone at the Circle features luxury apartments with refined details, exquisite dining, concierge services, and a dynamic lifestyle with art and cultural attractions just minutes away.

SCHEDULE YOUR VISIT TODAY.

617.996.7776


W WATERSTONE
AT THE CIRCLE

Now this is home.

CircleSeniorLiving.com

385 Chestnut Hill Avenue | Boston

  RELAY 711



With Suburban,
you're not just
a patient –
you're family.

With Suburban Home Health Care, you're not just a patient—you're family.

Family matters. And for more than 50 years, the Suburban Home Health Care family, which includes the Suburban Homemaking and Maternity Agency, has been providing expert in-home care for patients in a way that has consistently ranked them among the top in Massachusetts for quality of care, coverage area, languages spoken, and clinical capabilities.

- ✓ Skilled Nursing
- ✓ Physical Therapy
- ✓ Occupational Therapy
- ✓ Speech Therapy
- ✓ Home Health Aide Services
- ✓ Medicare and Medicaid Certified



SUBURBAN
HOME HEALTH CARE

suburbanhomehealth.com

(617) 264-7100

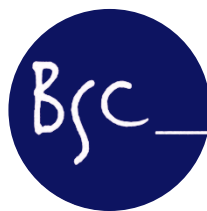
We are all stronger together

Beth Israel Deaconess Medical Center
joins the community in expressing our
appreciation to the Brookline Senior Center.
Thank you for keeping our seniors healthy.

Beth Israel Lahey Health



Beth Israel Deaconess
Medical Center



ADDING LIFE TO THE YEARS

Brookline Senior Center

93 Winchester Street, Brookline, MA 02446

617.730.2770 • brooklineseniorcenter.org